IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF 210 BLAKE STREET, APARTMENT #2, LEWISTON, MAINE	No. 2:24-mj-311-KFW

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Elliot Arsenault, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been since March 2022. I am currently assigned to HSI's Portland, Maine office. I have participated in numerous criminal investigations, to include matters involving investigations relating to the trafficking of narcotics. Through my training and experience, I have become familiar with the habits, methods, routines, practices, and procedures commonly employed by persons engaged in drug trafficking.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to search the residence located at 210 Blake Street, Lewiston, Maine being utilized by Target Subject MUKTAR ABSHIR ADEN a/k/a "Mo" (hereinafter "ADEN"). The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers, other agents, and witnesses. This affidavit is intended to provide the facts necessary for a determination of probable cause for the requested search warrant.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 841(a)(1) (Distribution or Possession with Intent to Distribute Controlled Substances) have been

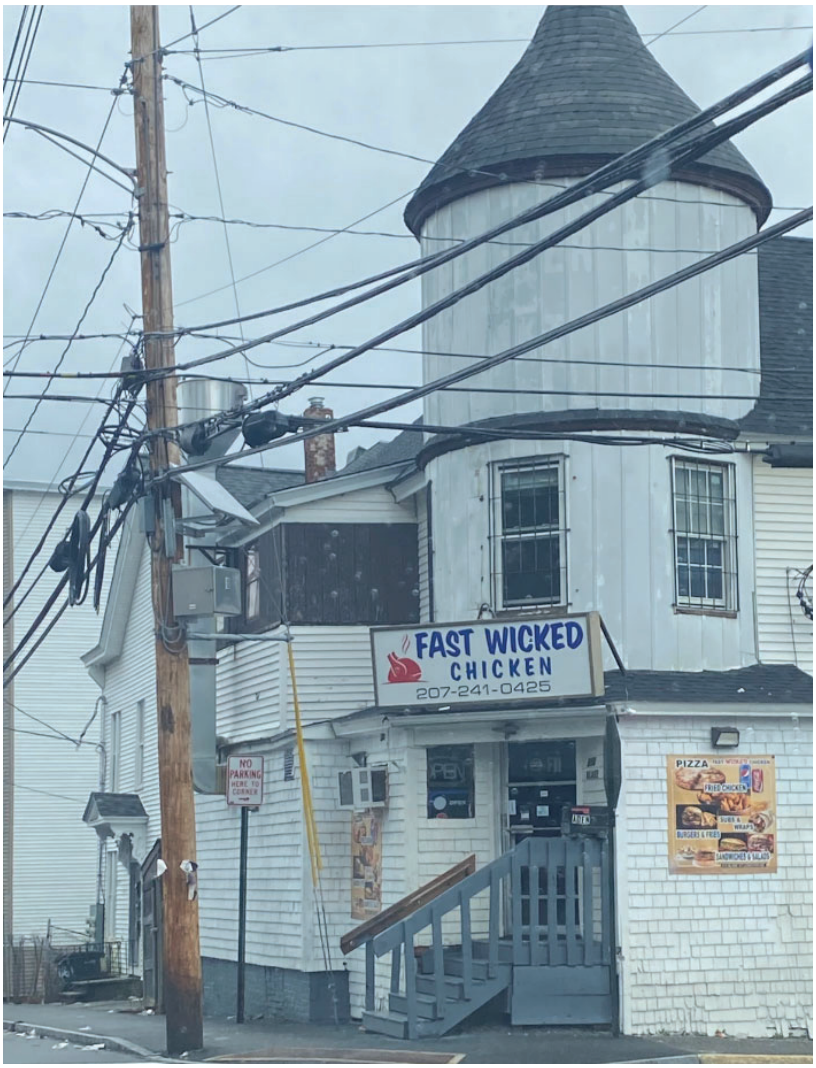
committed, are being committed, and will be committed by ADEN and his associates. There is probable cause to search the residence located at 210 Blake Street, Lewiston, Maine as described and depicted herein and in Attachment A for evidence and instrumentalities of these crimes as described in Attachment B.

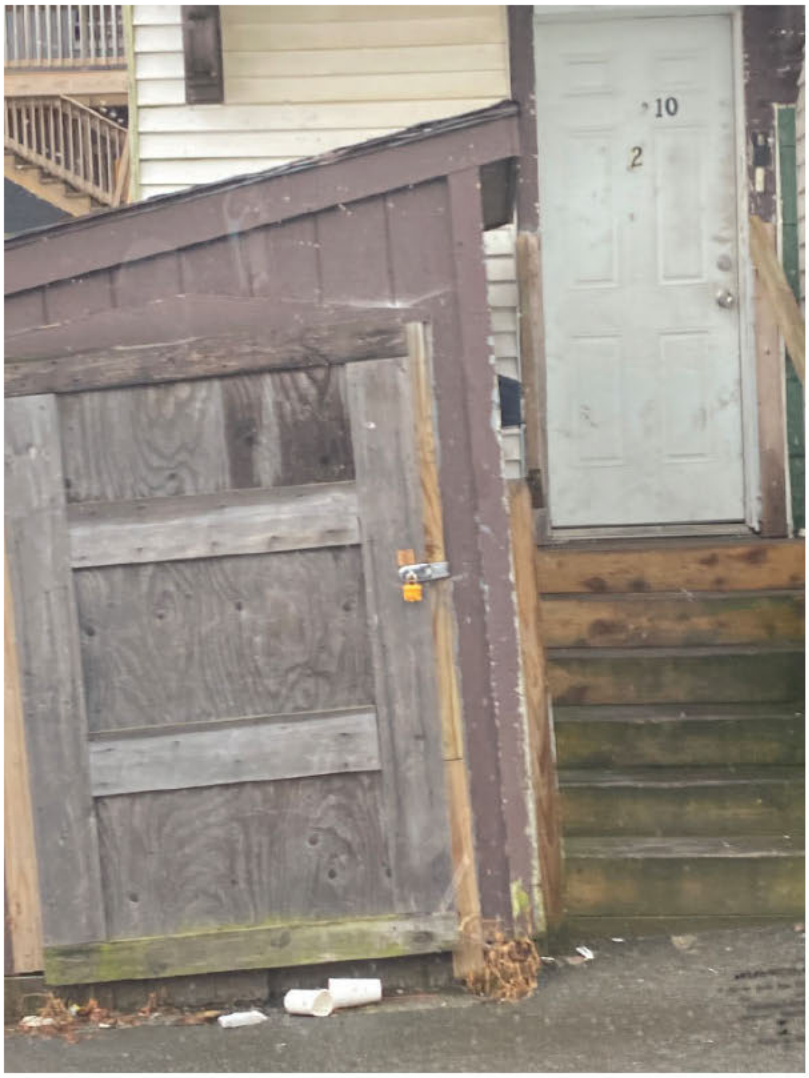
PLACE TO BE SEARCHED

As described and depicted herein and in Attachment A, this application is for a warrant to search the residence located at 210 Blake Street, Apartment #2, Lewiston, Maine ("the Target Residence"). The Target Residence is located in the city of Lewiston, Maine at the corner of Blake and Birch Street. The building is white in color and has a large turret or small tower on the second floor that overlooks the street side of the residence. The first floor is shingle siding and the second floor a vinyl clapboard siding. The property's first floor is occupied by a convenient food store named Fast Wicked Chicken. The entrance to the store is located at the corner of Blake and Birch Street, just below the turret.

The entrance to the second floor, known as apartment or unit 2, is located on the side of the building that faces Birch Street. The entrance door depicts the address of "210" and the number "2". A small wood staircase leads from the sidewalk to the door of apartment 2. In the rear of the building, apartment 2, can be reached from a pressure treated staircase. The staircase leads to a landing or deck, where the rear entrance door can be located. The building's roof is constructed with black or gray asphalt shingles.

The Target Residence is depicted below:


FAST WICKED
CHICKEN
207-241-0425
NO PARKING HERE TO CORNER
PIZZA



PROBABLE CAUSE

4. I hereby adopt and incorporate by reference my complaint affidavit filed in the United States District Court, District of Maine, Case No. 2:24-mj-310-KFW, attached hereto as Exhibit 1.

5. In addition to the controlled buy described in Exhibit 1, HSI and MDEA conducted additional controlled drug buys from ADEN using at least one confidential source of information. Five of these prior controlled buys took place at the Target Residence, beginning on August 19, 2024, and with the most recent buy at the Target

Residence occurring on September 18, 2024. Each of these buys was surveilled by agents and at least audio recorded, consistent with HSI protocol and as described in Exhibit 1.

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of

flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

7. Based on my training, experience, and research, I believe that electronic devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

8. As described above and in Attachment B, this application seeks permission to search for records that might be found at the Target Residence, in whatever form they

are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media (including cellular phones). Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

9. In my training and experience, individuals conduct a considerable amount of communication using their cellular telephones. Those communications are in the form of voice calls, text messages, SMS messages, MMS messages, e-mails, social media messages and posts, and messages shared via "chat" applications.

10. I know that individuals who conspire with one another to conduct illegal activities often do so through the use of cell phones and other electronic devices, used to communicate through social media and/or contact one another by voice or text messaging. I believe that a resident or residents (including ADEN) at the Target Residence and others (including drug suppliers and customers) would have communicated through such methods regarding drug trafficking. I know that individuals often utilize their cellular phones and smartphones to access the Internet and that each time this is done the device maintains a record or "browser history," showing which websites were visited and when.

11. I know from my training and experience, as well as through consultation with a trained cellular phone forensic analyst, that evidence of the above forms of communication, and the browser history of such devices, are often kept in cell phones for months and even years. I know that a forensic examiner may be able to recover messages and other data that were manually deleted by the user of the phone. For these reasons, I believe that any cellular phones and smartphones utilized by a resident or residents of the Target Residence will contain communications revealing a substantial

history of drug trafficking. For all those reasons, I request authorization to seize and search any cellular phones or smartphones found in the residence or on the person of ADEN, or on the persons of suspected drug suppliers or customers located at the Target Residence at the time of the search.

12. *Probable cause*. I submit that if a computer or storage medium is found at the Target Residence, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations,

artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

13. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

14. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Target Residence because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically

also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

15. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take

weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

16. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

17. Because several people may share the Target Residence, it is possible that the Target Residence will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless

determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

18. I submit that this affidavit supports probable cause for a search warrant and there is probable cause to believe that evidence and instrumentalities of these crimes, as described in Attachment B, are contained in the Target Residence described and shown in Attachment A.

Respectfully submitted,

Elliot W. Arsenault
Special Agent
Homeland Security Investigations

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedures

Date: Oct 08 2024

City and state: Portland, Maine

Judge's signature

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title